

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF GEORGIA  
SAVANNAH DIVISION

CR 422-0170

UNITED STATES OF AMERICA ) INDICTMENT NO.  
 )  
v. ) 18 U.S.C. § 1832(a)(5)  
 ) Conspiracy to Steal Trade Secrets  
JUAN MARTINEZ )  
 )

THE GRAND JURY CHARGES THAT:

At all times relevant to this Indictment:

1. Company A was a subsidiary of a publicly traded corporation whose business included the design, development, manufacturing, marketing and services of business jet aircraft. Company A sold and shipped jet aircraft, and intended to sell and ship jet aircraft, in the United States and internationally.

2. Company B was a publicly traded corporation whose business included the design, development, manufacturing, marketing and services of aircraft and aerospace technology.

3. Company C was a business that provided aviation related consulting services, which included designing airplane systems and providing engineering expertise.

Employment Background of Certain Co-Conspirators

4. From in or about October 2016 to November 29, 2018, Gilbert Basaldua ("Basaldua") was employed by Hi-Tek Professionals, Inc. as a contractor, and assigned to work as a numerical control engineer for Company A at one of its facilities in the Southern District of Georgia. In connection with his contract work for

Company A, Basaldua received training and signed agreements regarding the protection of proprietary information.

5. From on or about October 29, 2015 to November 17, 2016, and then again from June 20, 2017 to January 2, 2019, Defendant **JUAN MARTINEZ** was employed by third party contractors and assigned to work at Company B at one of its facilities outside the Southern District of Georgia. Most recently, Defendant **MARTINEZ** was assigned to work as a technical lead for a fire and safety group at Company B. In connection with his contract work for Company B and previous employment with other companies, Defendant **MARTINEZ** received training and signed agreements regarding the protection of proprietary information.

6. From on or about 2015 to in or about November 2018, Joseph Pascua ("Pascua") was employed by Company B to work as an engineer at Company B at one of its facilities outside the Southern District of Georgia. In connection with his employment with Company B, Pascua received training and signed agreements regarding the protection of proprietary information.

#### Co-Conspirators' Relationships With Company C

7. In approximately 2016, Pascua agreed to work with Company C to develop an aircraft wing anti-ice product (hereinafter "the product" or "Company C's product").

8. In approximately late 2016, Pascua invited Basaldua to work with Company C to develop the structural design of the product. Basaldua agreed to do so in exchange for a share of Company C's profits. Pascua and Basaldua also

collaborated with Craig German, who worked for another aircraft manufacturing company.

9. At no time did Basaldua notify his employer, Company A, of his conflicting relationship with Company C.

10. On or about December 15, 2017, Pascua filed a patent on behalf of Company C for the product. Pascua agreed with the owner and CEO of Company C that the two would share in any profits from sales of the product (hereinafter “Company C’s profits”).

11. In mid-2017, Pascua, Basaldua, and German recruited Defendant **JUAN MARTINEZ** to develop an icing/wind tunnel plan and model for use in testing Company C’s product. Defendant **MARTINEZ** agreed to do so in exchange for a share of Company C’s profits and other forms of payment.

Co-Conspirators’ Marketing and Development Efforts on Behalf of Company C

12. In 2017, Pascua, Basaldua, German and Defendant **MARTINEZ** presented Company C’s product to multiple aircraft companies to persuade them to invest in the product. While Company C’s concept was interesting, none of the aircraft companies would agree to invest in its development until, among other conditions, it was certified for flight in icing conditions by the Federal Aviation Administration (FAA). Company C’s product was not so certified.

13. Aircraft which were “certificated for flight in icing conditions” by the FAA went through an extensive procedure intended to ensure that they could safely operate throughout icing conditions encompassed by the icing envelopes specified by

the FAA. The icing certification process included extensive analysis, tunnel testing, dry-air testing, testing behind an icing tanker, and flight in natural icing conditions. The objective was to verify that the aircraft had functioning ice protection and to ensure that the aircraft would have acceptable performance and handling qualities in all the environmental conditions covered by the icing envelopes for which the aircraft had been tested.

14. To obtain FAA certification for the product, Pascua, Basaldua, German and Defendant **MARTINEZ** needed to develop an icing wind tunnel testing plan and submit the product to the rigorous process described above.

15. To shortcut the process of developing an original icing wind tunnel test plan, Pascua, Basaldua, German, and Defendant **MARTINEZ** agreed to steal proprietary aircraft wing schematics and anti-ice testing documents from other companies, to include Company A, and to use those documents without authority to develop an icing wind tunnel test plan for the product.

16. By utilizing proprietary aircraft wing schematics and anti-ice documents belonging to other aircraft companies, Pascua, Basaldua, German, and Defendant **MARTINEZ** understood that they could get the product to market faster and with far less expense to Company C.

#### The Stolen Proprietary Information

17. In particular, the proprietary information Defendant **MARTINEZ** and his cohorts planned to steal from Company A contained the following types of valuable and closely-guarded information regarding Company A aircraft:

- a. aircraft wing schematics, dimensions and detailed measurements;
- b. ice protection system designs, including bleed supply temperatures, mass flows and pressures;
- c. specific detail designs affecting the efficacy of aircraft ice protection and engine thrust;
- d. details regarding how to build an aircraft wing model for testing;
- e. certification testing conditions such as flight profiles, icing severity, system critical conditions, and angles of attack measurements;
- f. control temperatures relating to wing anti-icing and aircraft performance;
- g. step-by-step instructions for creating a certifiable anti-ice protection system throughout the entire icing envelope, to include descent and landing cases;
- h. individual finish and process codes unique to Company A;
- i. detailed test data, system performance and certification results from lab testing, icing tunnel tests, and dry air testing;

which information is hereinafter referred to as, “anti-ice and wing model information.”

18. The anti-ice and wing model information described above was considered trade secret information by Company A.

19. Company A protected its anti-ice and wing model information as confidential and proprietary. Company A used a number of reasonable measures to protect its sensitive and proprietary information, including the following:

- a. Company A staffed guards in its main lobby during business hours and deployed a mobile patrol unit to conduct routine patrols 24-hours per day, 7 days per week.

- b. Company A granted physical access to its facilities to only those persons with a valid badge. Company A required all employees, contractors and visitors to have a badge and wear it visibly at all times. Badges could be used to access only those areas that an employee or contractor had a predetermined need to access.
- c. To sponsor a visitor and obtain a visitor badge, a Company A employee had to submit a visitor request including the visitor's name, company affiliation, purpose for visit and citizenship status. Citizenship status information was required because certain areas of Company A are off limits to non-U.S. nationals.
- d. Company A maintained visitor logs in its badging system and required that visitors be escorted by Company A personnel at all times while in the facility.
- e. Company A implemented data security policies by requiring all new employees and contractors to sign declarations that they have read, reviewed, and agree to abide by Company A's Business Conduct and Ethics Policy, as well as its Use of Computing Systems, Equipment and Support policy. These policies prohibited the unauthorized use or dissemination of sensitive and proprietary information, as well as the use of storage devices and laptops on its computer systems and networks without authorization. Company A confidentiality obligations continue even after an employee or contractor leaves Company A.
- f. Company A employees with access to information about Company A's future programs and activities which had not yet been announced company-wide were required to sign an additional Need To Know document in which they agreed to maintain the confidentiality of that information, even from other Company A employees.
- g. Company A required suppliers, vendors and service providers to execute proprietary information/non-disclosure agreements before they were allowed to receive any Company A confidential and proprietary information or access Company A facilities.
- h. Company A limited access to its sensitive and proprietary information to those who needed the information to perform their employment duties on Company A's secure electronic database. To obtain access to this database,

employees were required to: (1) possess a valid employee badge to enter Company A's main buildings; (2) swipe the badge to access limited-access areas; (3) scan the badge into an employee computer terminal; (4) login with a unique username and password to the Company A network; (5) open a database to which a limited number of employees had access; and (6) login to the database with a unique employee number and password.

- i. Company A tracked searches within its database, such that a system administrator could see what a unique user has searched for and accessed, as well as when the activity occurred.
- j. Company A labeled the front of its reports with a notice indicating that the information was proprietary and that the information could not be disclosed to others without the written authorization of Company A.
- k. Company A prohibited remote access to its database without an approved Company A laptop or cellphone and a VPN token to ensure an encrypted connection.

COUNT ONE  
*Conspiracy*  
18 U.S.C. § 1832(a)(5)

Beginning on a date unknown to the grand jury, but at least by in or about October 2017, and continuing until on or about January 2019, within the Southern District of Georgia, and elsewhere, the defendant,

**JUAN MARTINEZ,**

and others known and unknown to the grand jury, aided and abetted by each other, with some joining the conspiracy earlier and others joining later, did knowingly and willfully combine, conspire, confederate, agree with each other, and others known and unknown to the grand jury, to commit the following offenses:

- a. With intent to convert a trade secret that is related to a product that is



used in and intended for use in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will injure any owner of that trade secret, knowingly steal and without authorization appropriate, take, carry away and conceal, and by fraud, artifice, and deception obtain such information, in violation of Title 18, United States Code, Section 1832(a)(1);

- b. With intent to convert a trade secret that is related to a product that is used in and intended for use in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will injure any owner of that trade secret, knowingly, and without authorization copy, duplicate, sketch, draw, photograph, download, upload, alter, destroy, photocopy, replicate, transmit, deliver, send, mail, communicate, and convey such information, in violation of Title 18, United States Code, Section 1832(a)(2); and
- c. With intent to convert a trade secret that is related to a product that is used in and intended for use in interstate and foreign commerce, to the economic benefit of anyone other than the owner of the trade secret, and intending and knowing that the offense will injure any owner of that trade secret, knowingly receive, and possess such information, knowing the same to have been stolen and appropriated, obtained, and converted



without authorization, in violation of Title 18, United States Code, Section 1832(a)(3).

Manner and Means

20. Defendant **MARTINEZ**, Basaldua, Pascua, and German would and did carry out the conspiracy and its unlawful objects, that is the theft, unauthorized taking, carrying away, concealment, copying, download, upload, replication, transmission, delivery, sending, communicating, and conveying, receipt, and possession of anti-ice and wing model information owned and controlled by Company A through the following manner and means, among others:

- a. It was part of the conspiracy that Defendant **MARTINEZ**, Basaldua, Pascua, and German planned to take, without authority, proprietary documents and engineering drawings from Company A, which documents contained information that was considered by Company A to be trade secrets.
- b. It was further part of the conspiracy that Defendant **MARTINEZ**, Basaldua, Pascua, and German planned to utilize Company A's proprietary information, without authority, to create a test plan and test model for conducting icing wind tunnel testing to obtain Federal Aviation Administration (FAA) certification for Company C's aircraft wing anti-ice product.
- c. It was further part of the conspiracy that Defendant **MARTINEZ** would provide search terms to Basaldua to assist Basaldua in searching

Company A systems for its proprietary documents and engineering drawings related to anti-ice test plans and test models.

- d. It was further part of the conspiracy that Basaldua would search internal Company A networks for anti-ice documents, engineering schematics and aircraft wing drawings.
- e. It was further part of the conspiracy that Basaldua would download and print Company A's anti-ice documents, engineering schematics and aircraft wing drawings.
- f. It was further part of the conspiracy that Basaldua would change the file names of Company A's electronic files to conceal their true nature.
- g. It was further part of the conspiracy that Basaldua would email stolen Company A documents from his Company A email account to his personal Yahoo email account.
- h. It was further part of the conspiracy that Basaldua would create scanned electronic copies of stolen Company A documents using commercial copy equipment.
- i. It was further part of the conspiracy that Basaldua would store electronic copies of stolen Company A documents on his personal electronic storage devices.
- j. It was further part of the conspiracy that Basaldua would store hard copies of stolen Company A and other aircraft companies' proprietary documents in his residence.

- k. It was further part of the conspiracy that Basaldua would mail or electronically send stolen Company A proprietary material to Defendant **MARTINEZ** and the other co-conspirators.
- l. It was further part of the conspiracy that Defendant **MARTINEZ** and his co-conspirators would share a cloud-based storage account to store and share proprietary information related to development of the aircraft anti-ice technology, to include proprietary information stolen from Company A.
- m. It was further part of the conspiracy that Defendant **MARTINEZ**, Pascua, and Basaldua would utilize Company A's stolen proprietary engineering schematics, measurements, dimensions, and drawings to design and attempt to design a test article for the co-conspirators and Company C.
- n. It was further part of the conspiracy that Defendant **MARTINEZ** would utilize Company A's stolen proprietary information to create and attempt to create an icing wind tunnel test plan, with the intent to use the icing wind tunnel test plan to obtain FAA certification for Company C's product.
- o. It was further part of the conspiracy that Defendant **MARTINEZ** would reserve time at icing wind tunnel testing facilities with the intent to test Company C's product, which tests the co-conspirators knew would utilize Company A's proprietary information.

21. In furtherance of the conspiracy and to achieve the objects and purposes thereof, Defendant **MARTINEZ**, Basaldua, Pascua, and German committed and caused to be committed the following overt acts, among others, in the Southern District of Georgia and elsewhere:

- a. On or about March 21, 2018, Defendant **MARTINEZ** instructed Basaldua via text message to search Company A's internal systems for the "Anti Ice certification plan" of a particular Company A model aircraft.
- b. On or about March 23, 2018, Basaldua utilized terms relating to anti-ice to search internal Company A systems.
- c. On or about March 23, 2018, Basaldua used Company A internal systems to view and attempt to view a Company A anti-ice document.
- d. On or about March 27, 2018, Basaldua utilized terms relating to anti-ice to search internal Company A systems.
- e. On or about March 27, 2018, Basaldua used Company A internal systems to view and attempt to view approximately 13 Company A anti-ice documents.
- f. On or about March 27, 2018, Basaldua viewed and downloaded, from Company A's internal system, a Company A proprietary anti-ice document ending in 1875.
- g. On or about March 27, 2018, Basaldua sent a text message to J.M. stating, "I believe I found the test plan."
- h. On or about March 27, 2018, Basaldua emailed Defendant **MARTINEZ**,

Pascua, and German a Company A proprietary anti-ice document ending in 1875 with a message stating, "Here you go guard this, my job depends on it."

- i. On or about March 27, 2018, Pascua sent Defendant **MARTINEZ** and Basaldua a text message that said, "I'm also setting a conference call for APAC with Tony for tomorrow, March 28, 8:30 pm EST. He said he has new info on the Chinese investment for the ice tunnel test."
- j. On or about April 6, 2018, Defendant **MARTINEZ** sent Basaldua an email with an attachment titled, "Anti-Ice\_Plan.docx," which was a preliminary draft of Company C's icing tunnel test plan. In the email, Defendant **MARTINEZ** stated, "I still need a lot of information."
- k. On or about April 12, 2018, Defendant **MARTINEZ** asked Basaldua via text message to search Company A internal systems for information pertaining to "cabin pressurization system," "outflow valve," or "outflow valve system."
- l. On or about April 13, 2018, Basaldua sent Defendant **MARTINEZ** the title of a Company A document via text message, but stated, "I am not allowed access."
- m. On or about April 13, 2018, Basaldua informed Defendant **MARTINEZ** via text message, "I should have what you need. 6 docs about 300 pages. Should be somewhere in there."
- n. On or about April 13, 2018, Defendant **MARTINEZ** replied via text

message, "Cool Please mail it here," and provided his mailing address.

- o. On or about June 21, 2018, Defendant **MARTINEZ** sent a text message to Basaldua and Defendant **PASCUA** reading, "Gilbert I need a couple of documents. I'll send the numbers in a few."
- p. On or about June 21, 2018, Basaldua replied to Defendant **MARTINEZ**, "Ok," after which Defendant **MARTINEZ** sent Basaldua the names of two Company A proprietary documents ending in 1874 and 1219.
- q. On or about June 22, 2018, Basaldua accessed Company A internal systems and viewed a Company A proprietary anti-ice document ending in 1874.
- r. On or about June 22, 2018, Basaldua told Defendant **MARTINEZ**, via text message, "Got both docs."
- s. On about June 24, 2018, Basaldua visited a commercial copying business in Hilton Head, SC, and created a scanned copy of a Company A proprietary anti-ice document, the document number of which ended in 1874.
- t. On or about June 24, 2018, Basaldua emailed Company A's proprietary anti-ice document ending in 1874 to Defendant **MARTINEZ** as an attachment titled, "Staples Scan.pdf."
- u. On or about November 12, 2018, Defendant **MARTINEZ** asked Basaldua via email to obtain specific Company A proprietary documents ending in 0498 and 1290.

- v. On or about November 19, 2018, Basaldua sent a text message to Defendant **MARTINEZ** and Pascua, notifying them that he had uploaded a Company A proprietary ice tunnel testing document to a cloud storage space for them to view.
- w. On or about November 21, 2018, Basaldua sent an email from his Company A email account to his personal Yahoo account titled, "Time Card," with an attachment titled, "Wing.ppt." The attachment titled, "Wing.ppt" contained a PowerPoint file with engineering drawings of a Company A aircraft wing.
- x. Between on or about November 13-28, 2018, Basaldua accessed internal Company A systems to view and attempt to view multiple Company A proprietary anti-ice documents and wing drawings.
- y. On or about November 13, 2018, Basaldua accessed internal Company A systems to view a Company A proprietary anti-ice document ending in 1290.
- z. Between on or about November 13-27, 2018, Basaldua downloaded the Company A proprietary anti-ice document ending in 1290 and changed the file name to "Time Card."
- aa. On or about November 27, 2018, Basaldua emailed the Company A proprietary anti-ice document ending in 1290, now titled, "Time Card," from his Company A email account to his personal Yahoo account.
- bb. On or about November 28, 2018, Basaldua emailed Pascua a file with



filename ending in 0010.CATPART, which file contained wing prints that had been taken without authority from Company A.

All in violation of Title 18, United States Code, Section 1832(a)(5).

### **FORFEITURE ALLEGATIONS**

The allegations contained in Count One of this Indictment are hereby re-alleged and incorporated by reference for the purpose of alleging forfeiture pursuant to Title 18, United States Code, Sections 981, 2323, and Title 28, United States Code, Section 2461.

22. Upon conviction of Title 18, United States Code, Section 1832(a)(5), set forth in Count One of this Indictment, the Defendant,

**JUAN MARTINEZ,**

shall forfeit to the United States pursuant to Title 18, United States Code, Section 2323, any article, the making or trafficking of which is prohibited, and any property used, or intended to be used in any manner or part to commit or facilitate the commission of prohibited activity, as well as any property constituting or derived for any proceeds obtained directly or indirectly as a result of the commission of the prohibited activity, and pursuant to Title 18, United States Code, Section 981(a)(1)(C), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense.

23. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty,

the United States of America shall be entitled to forfeiture of substitute property pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c).



David H. Estes  
United States Attorney

Patricia G. Rhodes  
Assistant United States Attorney  
Chief, Criminal Division

Jennifer G. Solari  
Assistant United States Attorney  
Senior Litigation Counsel  
\*Lead Counsel

Darron J. Hubbard  
Assistant United States Attorney  
\*Co-lead Counsel